UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

NANCY RANDALL, individually and on behalf of all others similarly situated, Plaintiff, v. MR. COOPER GROUP, INC., Defendant.	Civil Action No. 3:23-cv-02507 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, Nancy Randall, on behalf of herself and all persons similarly situated, alleges:

NATURE OF THE CASE

1. This is a consumer class action lawsuit brought by Plaintiff, individually and on behalf of all others similarly situated (i.e., the Class Members), who entrusted Defendant Mr. cooper Group, Inc. ("Mr. Cooper" or "Defendant"), to safeguard their personally identifiable information ("PII"), which includes, without limitation, names, addresses, Social Security numbers and dates of birth.

2. Defendant has failed to comply with industry standards to protect information in its systems that contain PII, and has failed to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their PII had been compromised. Plaintiff seeks, among other things, orders requiring Defendant to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably sufficient security practices and safeguards to prevent incidents like this in the future.

3. Defendant experienced a data security incident purportedly discovered by Defendant on "October 31, 2023", in which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed highly sensitive PII that was being kept unprotected ("Data Breach"). As a result, an unauthorized party accessed certain files and folders within the Defendant's systems and may have viewed, acquired, and/or exfiltrated data containing affected parties' PII. The security incident was wide-reaching, impacting a number of the Defendant's computer systems and compromising the PII of millions of people.

4. As a result of Defendant's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII is now in the hands of criminals. Plaintiff and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to the Defendant's failures.

5. Accordingly, Plaintiff, individually and on behalf of all others similarly situated, alleges claims for negligence and negligence *per se*, breach of implied contract, unjust enrichment, injunctive/declaratory relief and Violation of Washington Consumer Protection Act, Wash. Rev. Code §§ 19.86.020, *et seq.*

PARTIES

6. Plaintiff Nancy Randall lives in Deer Park, Washington and is a resident and citizen of the State of Washington. Plaintiff holds a mortgage that is serviced by Defendant. Plaintiff's PII was collected and maintained by Defendant and disclosed without authorization to an unknown and unauthorized third party as a result of the Data Breach.

7. Defendant is a Texas corporation with a principal place of business located at 8950 Cypress Waters Blvd. Coppell, TX 75019. The registered agent for service of process is

Corporation Service Company d/b/a CSC - Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, TX 78701-3218.

8. According to Inside Mortgage Finance, Mr. Cooper Group, Inc., is the third largest mortgage servicer in the United States, with 4.3 million customers nationwide.[1]

9. Due to the nature of the services it provides, Defendant regularly acquires and electronically stores PII belonging to consumers as part of the regular course of its business.

JURISDICTION AND VENUE

10. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant.

11. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

12. Defendant is headquartered and has its principal place of business of and/or routinely conducts business in the Dallas Division of the Northern District of Texas, has sufficient minimum contacts in this State, has intentionally availed itself of this jurisdiction by marketing and/or selling products and/or services and/or by accepting and processing payments for those products and/or services within this State.

13. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of

[1] MR. COOPER, OVERVIEW: https://www.mrcooper.com/about-us/overview (last accessed November 8, 2023).

the events that gave rise to Plaintiff's claims took place within the Dallas Division of the Northern District of Texas and Defendant is headquartered and/or does business in the Dallas Division of the Northern District of Texas.

BACKGROUND AND FACTS

14. According to Defendant, the Data Breach occurred on October 31, 2023, when Mr. Cooper became the target of a cyber security incident.

15. Plaintiff was provided the information detailed above upon receipt of an e-mail from Defendant. Plaintiff was not aware of the Data Breach until receiving this e-mail.

16. The email is deficient, failing to provide basic details concerning the Data Breach, including, but not limited to, why sensitive information was stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the stolen data was encrypted or otherwise protected, and whether Defendant knows if the data has not been further disseminated.

17. Defendant acknowledges that it is responsible to safeguard Plaintiff and Class Members' PII and promises to protect the security and privacy of PII.

18. Defendant's customers entrusted their PII to Defendant with the mutual understanding that this highly sensitive private information was confidential and would be properly safeguarded from misuse and theft.

19. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and Class Members' PII from disclosure.

20. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and they rely on Defendant to keep this information confidential and

securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

21. Defendant was well aware that the PII it collects is highly sensitive and of significant value to those who would use it for wrongful purposes. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and fraud.[2] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the dark web.

22. The ramifications of Defendant's failure to keep PII secure are long lasting and severe. Once stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

23. Further, criminals often trade stolen PII on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publicly available.

24. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[3] This time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used, compounds an identity theft victim's ability to detect and address the harm.

---

[2] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Sept. 25, 2023).

[3] *Identity Theft and Your Social Security Number*, Social Security Administrative, *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Sept. 25, 2023).

25. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

26. Further, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

27. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[4]

28. Defendant knew, or should have known, the importance of safeguarding PII entrusted to it and of the foreseeable consequences if its systems were breached. This includes the significant costs that would be imposed on individuals as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

[4] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Sept. 25, 2023).

29. Plaintiff and Class Members now face years of constant surveillance of their records. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

30. Despite all of the publicly available knowledge of the continued compromises of PII, Defendant's approach to maintaining the privacy of the PII was lackadaisical, cavalier, reckless, or in the very least, negligent.

31. In all contexts, time has constantly been recognized as compensable, and for many people, it is the basis on which they are compensated. Plaintiff and Class Members should be spared having to deal with the consequences of Defendant's misfeasance.

32. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.

33. The delay in identifying and reporting the Data Breach caused additional harm to Plaintiff and Class Members, depriving them of the ability to promptly mitigate potential adverse resulting consequences.

34. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at increased risk of suffering:

a. Actual identity theft;

b. Unauthorized use and misuse of their PII;

c. The loss of the opportunity to control how their PII is used;

d. The diminution in value of their PII;

e. The compromise, publication, and/or theft of their PII;

f. Out-of-pocket costs associated with the prevention, detection, recovery and

remediation from identity theft or fraud;

g. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

h. Costs associated with placing freezes on credit reports;

i. Delay in receipt of tax refund monies or lost opportunity and benefits of electronically filing of income tax returns;

j. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

k. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as it fails to undertake appropriate measures to protect the PII in its possession; and

l. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

35. To date, Defendant has not yet disclosed full details of the Data Breach. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, taken to secure the PII still in its possession. Through this litigation, Plaintiff seeks to determine the scope of the Data Breach and the information involved, obtain relief that redresses any harms, and ensure Defendant has proper measures in place to prevent another breach from occurring in the future.

36. Defendant was expressly prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

37. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[5]

38. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[6] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

39. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

40. Defendant failed to properly implement basic data security practices. This failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

41. Defendant was at all times fully aware of its obligation to protect PII and was also aware of the significant repercussions that would result from its failure to do so.

---

[5] Federal Trade Commission, *Start With Security: A Guide for Business*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Sept. 25, 2023).

[6] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Sept. 25, 2023).

Plaintiff's Experience

42. On or about November 2, 2023, Plaintiff was notified via e-mail from Defendant that her PII had been accessed because of the Data Breach.

43. Plaintiff is an adult individual and, at all times relevant herein, a resident and citizen of the State of Washington. Plaintiff is a victim of the Data Breach.

44. Defendant received Plaintiff's PII in connection with financial services rendered to her by Defendant through Plaintiff's mortgage.

45. As a result, Plaintiff's information was among the data an unauthorized third party accessed in the Data Breach. It is unclear from the lack of sufficient notice by the Defendant the specifics of what part of her personal identifiable information in the possession of the Defendant was compromised due to its negligence.

46. Plaintiff is very careful about sharing and protecting her PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted her PII to Defendant had she known of Defendant's lax data security policies.

47. As a result of the Data Breach, and at the direction of Defendant's email, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach. She regularly monitors her credit through multiple services and has undertaken efforts to immediately do so as a result of the Data Breach. She is now considering taking additional steps to protect her exposed PII, including paying for a credit monitoring service, changing passwords and resecuring her own computer network, and checking her personal and financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach–valuable time Plaintiff otherwise would have spent on other activities, including but not

limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

48. Plaintiff has suffered injury because her personal information is likely now on the dark web as a result of the Defendant's negligence. In addition to the time and efforts undertaken as set forth above, she has experienced an increase in spam phone calls, which, upon information and belief, was caused by the Data Breach and only began following the Data Breach. Upon information and belief, was caused by the Data Breach and only began following the Data Breach.

49. Plaintiff suffered actual injury and fraud from having her PII compromised as a result of the Data Breach including, but not limited to: (i) lost or diminished value of her PII; (ii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) invasion of privacy; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

50. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

51. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

52. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

53. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future

breaches.

CLASS ACTION ALLEGATIONS

54. Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure ("F.R.C.P.") on behalf of herself and all others similarly situated (the "Class"). Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All individuals in the United States whose PII was maintained by Defendant and who were sent a notice regarding the Data Breach.**

Plaintiff also brings her claims on behalf of a subclass of Washington victims ("Washington Subclass"), defined as follows:

> **All individuals in Washington whose PII was maintained by Defendant and who were sent a notice regarding the Data Breach.**

55. Excluded from the Class are Defendant, Defendant's subsidiaries and affiliates, officers, directors, IT employees and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representatives, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

56. Plaintiff reserves the right to modify or amend the definition of the proposed Class and Subclass and/or to add classes or subclasses, if necessary, before this Court determines whether certification is appropriate.

57. Numerosity: The Class Members are so numerous that joinder of all Members is impractical. The Class is comprised of potentially millions of individuals. Defendant has the administrative capability through its computer systems and other records to identify all members

of the Class and Subclass, and such specific information is not otherwise available to Plaintiff.

58. Commonality: The questions here are ones of common or general interest such that there is a well-defined community of interest among the Members of the Class and Subclass. These questions predominate over questions that may affect only individual class members because Defendant has acted on grounds generally applicable to the Class and Subclass. Such common legal or factual questions include, but are not limited to:

a. Whether and to what extent Defendant had a duty to protect the PII of Class Members;

b. Whether Defendant were negligent in collecting and storing Plaintiff's and Class Members' PII;

c. Whether Defendant had duties not to disclose the PII of Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;

e. Whether Defendant failed to adequately safeguard the PII of Class Members;

f. Whether Defendant breached duties to exercise reasonable care in handling Plaintiff's and Class Members' PII;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

i. Whether Plaintiff and Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach; and

o. Whether Plaintiff and Class Members are entitled to additional identity theft protection.

59. Typicality: Plaintiff's claims are typical of the claims of the other members of the Class because Plaintiff's PII, like that of every other Class Member, was not properly maintained or secured by Defendant. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

60. It is impracticable to bring the individual claims of the members of the Class and Subclass before the Court. Class treatment permits a large number of similarly situated persons or entities to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort, expense, or the possibility of inconsistent or contradictory judgments that numerous individual actions would engender. The benefits of the class mechanism, including providing injured persons or entities with a method for obtaining redress on claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in the management of this class action.

61. Adequacy of Representation: Plaintiff is a more than adequate representative of the Class in that Plaintiff's PII was compromised and has suffered damages. In addition:

a. Plaintiff is committed to the vigorous prosecution of this action on behalf of herself and all others similarly situated and has retained competent counsel experienced in the prosecution of class actions and, in particular, class actions regarding data breaches;

b. There is no conflict of interest between Plaintiff and the unnamed members of the Class or Subclass;

c. Plaintiff anticipates no difficulty in the management of this litigation as a class action; and

d. Plaintiff's legal counsel have the financial and legal resources to meet the substantial costs and legal issues associated with this type of litigation.

62. Plaintiff knows of no difficulty to be encountered in the maintenance of this action that would preclude its maintenance as a class action.

63. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

64. Defendant has acted or refused to act on grounds generally applicable to the Class and Subclass, thereby making appropriate corresponding declaratory relief with respect to the Class and Subclass as a whole. Defendant's actions and inactions challenged herein apply to and affect Class Members uniformly and hinges on its conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

65. Superiority of Class Action. Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against a large organization like Defendant. Further, even for

those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

66. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

67. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

68. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

69. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and may continue to act unlawfully as set forth in this Complaint.

70. All conditions precedent to bringing this action have been satisfied and/or waived.

FIRST CAUSE OF ACTION
Negligence and Negligence *Per Se*
(On Behalf of Plaintiff and the Classes)

71. Plaintiff and the Class re-allege and incorporate by reference each and every preceding paragraph of this Complaint.

72. Defendant requires its customers, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of providing services.

73. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of its business, which affects commerce.

74. Plaintiff and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

75. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

76. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.

77. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

78. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

79. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed with Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of being customers of Defendant.

80. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

81. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

82. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' Private Information it was no longer required to retain pursuant to regulations.

83. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

84. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

85. Defendant breached its duties, pursuant to the FTC Act, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to remove former customers' Private Information it was no longer required to retain pursuant to regulations; and

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

86. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

87. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

88. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

89. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

90. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

91. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial and mortgage related industries.

92. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

93. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

94. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

95. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

96. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

97. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

98. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

99. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

100. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

101. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) and increase in spam calls, texts, and/or emails; and (vi) the continued and certainly

increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

102. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

103. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

104. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

105. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

106. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Classes)

107. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein.

108. When Plaintiff and members of the Class provided their personal information to Defendant or its corporate partners, Plaintiff and Class Members entered into implied contracts pursuant to which it agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their data had been breached and compromised.

109. Defendant's impugned or actual implied promises to Plaintiff and Class members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to PII also protect the confidentiality of that data; (2) taking steps to ensure that the PII that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the PII against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

110. Defendant or its corporate partners required Plaintiff and Class Members to provide and entrust their PII as a condition of obtaining services.

111. Plaintiff and Class Members would not have provided and entrusted their PII and in the absence of the implied contract between them and Defendant or its corporate partners.

112. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant or its corporate partners.

113. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect the personal information of Plaintiff and Class Members and by failing to provide timely and accurate notice to them that their personal information was compromised in and as a result of the Data Breach.

114. The losses and damages sustained by Plaintiff and Class members as described herein were the direct and proximate result of Defendant's breaches of the implied contracts between it and Plaintiff and Class Members.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Classes)

115. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein.

116. This cause of action is brought in the alternative to Plaintiff's breach of contract cause of action. If claims for breach of contract are ultimately successful, this cause of action will be dismissed.

117. Plaintiff and Class Members conferred a benefit on Defendant by way of customers' paying Defendant or its corporate partners to maintain Plaintiff and Class Members' PII.

118. The monies paid to Defendant were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and Class Members.

119. Defendant failed to provide reasonable security, safeguards, and protections to the personal information of Plaintiff and Class Members, and as a result Defendant was overpaid.

120. Under principles of equity and good conscience, Defendant should not be permitted to retain the money because Defendant failed to provide adequate safeguards and security

measures to protect Plaintiff's and Class Members' personal information that they paid for but did not receive.

121. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

122. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

123. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

FOURTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Classes)

124. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein.

125. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

126. An actual controversy has arisen after the Data Breach regarding Plaintiff's and Class Members' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff continue to suffer injury due to the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

127. Plaintiff and the Classes have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including: (i) Defendant's failure to encrypt Plaintiff's and Class Members' PII, including Social Security numbers, while storing it in an Internet-accessible environment, and (ii) Defendant's failure to delete PII it has no reasonable need to maintain in an Internet-accessible environment, including the Social Security numbers of Plaintiff.

128. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PII of Plaintiff and Class Members;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII;

c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiff harm.

129. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law, industry, and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendant to:

a. engage third-party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test its systems for security vulnerabilities, consistent with industry standards; and

d. implement an education and training program for appropriate employees regarding cybersecurity.

130. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff will not

have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

131. The hardship to Plaintiff, if an injunction is not issued, exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to use such measures.

132. Issuance of the requested injunction will satisfy the public interest. On the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and others whose confidential information would be further compromised.

FIFTH CAUSE OF ACTION
VIOLATION OF WASHINGTON CONSUMER PROTECTION ACT,
Wash. Rev. Code §§ 19.86.020, *et seq.*
(On Behalf of Plaintiff and the Washington Subclass)

133. Nancy Randall, the Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclass, repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

134. Defendant is a "person," as defined by Wash. Rev. Code § 19.86.010(1).

135. Defendant advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code § 19.86.010 (2).

136. Defendant engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code § 19.86.020, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

137. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of customers' PII.

138. Defendant acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff and Washington Subclass Members' rights. Defendant was on notice that its security and privacy protections were inadequate.

139. Defendant's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons.

140. Further, its conduct affected the public interest, including the many Washingtonians affected by the Data Breach.

141. As a direct and proximate result of Defendant's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Washington Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

142. Plaintiff and Washington Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all other similarly situated, prays for relief as follows:

A. For an order certifying the Class and Subclass and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

C. For compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;

D. For an order of restitution and all other forms of equitable monetary relief;

E. Declaratory and injunctive relief as described herein;

F. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

G. Awarding pre- and post-judgment interest on any amounts awarded; and

H. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Date: November 10, 2023

Respectfully submitted,

/s/ Joe Kendall
JOE KENDALL
Texas State Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suiet 825
Dallas, Texas 75219
Telephone: (214) 744-3000
Facsimile: (214) 744-3015
jkendall@kendalllawgroup.com

Kenneth Grunfeld*
KOPELOWITZ OSTROW, P.A.
65 Overhill Road
Bala Cynwyd, Pennsylvania 19004
Main: 954-525-4100
grunfeld@kolawyers.com

Attorneys for Plaintiff and Proposed Class

**Pro hac vice forthcoming*